

Listing of Claims:

Claims 1-47 (cancelled).

Claim 48: (Previously Presented) An apparatus comprising:

a processor configured to:

generate an electronic ticket for providing an electronic key device authorization to unlock an electronic lock device, the electronic ticket comprising a public key corresponding to the electronic key device and a link key configured to authenticate an identity of the electronic lock device,

wherein the apparatus is authorized to unlock the electronic lock device,

wherein the ticket is transmittable from the apparatus to the electronic key device and wherein the ticket is electronically signed by the apparatus using a private key of the apparatus,

wherein the public key corresponding to the electronic key device is configured to decrypt a code issued by the electronic lock device and encrypted by the electronic key device, and

wherein the link key of the electronic ticket is generated using a one-way hash of a link key of the apparatus and a lock identifier of the electronic lock device.

Claim 49: (Previously Presented) The apparatus according to claim 48, wherein the processor is further configured to wirelessly communicate using Bluetooth short range communication protocol.

Claim 50: (Previously Presented) The apparatus according to claim 48, wherein said electronic lock device is a virtual lock device in a form of a software module controlling access to a digital resource.

Claim 51: (Previously Presented) The apparatus according to claim 48, wherein said electronic lock device stores public keys for a plurality of authorized key holders.

Claim 52: (Previously Presented) The apparatus according to claim 48, wherein the public key is stored in a plurality of lock devices for which entry is authorized for the apparatus.

Claim 53: (Previously Presented) The apparatus according to claim 48, wherein a different public key is stored in each lock device for which entry is authorized for the apparatus.

Claim 54: (Previously Presented) The apparatus according to claim 48, wherein at least one of the apparatus and the electronic key device comprises a portable wireless device.

Claim 55: (Previously Presented) The apparatus according to claim 54, wherein at least one of the apparatus and the electronic key device comprises a wireless telephone.

Claim 56: (Previously Presented) The apparatus according to claim 54, wherein at least one of the apparatus and the electronic key device is wearable by a user.

Claim 57: (Previously Presented) The apparatus according to claim 48, wherein the apparatus further comprises a power source, non-volatile memory and a transmitter/receiver unit.

Claim 58: (Previously Presented) The apparatus according to claim 57, wherein at least one of the apparatus and the electronic key device further includes a user authentication device.

Claim 59: (Previously Presented) An apparatus comprising:

a processor configured to:

receive at least one electronic ticket transmitted from an electronic key device authorized to unlock an electronic lock device, wherein the at least one received electronic ticket comprises a public key corresponding to the apparatus and a link key configured to authenticate an identity of the electronic lock device, wherein the link key of the electronic ticket is generated using a one-way hash of a link key of the electronic key device and a lock identifier of the electronic lock device,

transmit the at least one electronic ticket to the electronic lock device,

receive a code issued by the electronic lock device,
encrypt the code using a private key of the apparatus, and
transmit the encrypted code to the electronic lock device, wherein the public key
of the apparatus is configured to decrypt the encrypted code.

Claim 60: (Previously Presented) The apparatus according to claim 59, wherein said
electronic lock device is a virtual lock device in a form of a software module controlling access
to digital resources.

Claim 61: (Previously Presented) The apparatus according to claim 60, wherein the at least
one electronic ticket grants access to at least part of said digital resources.

Claim 62: (Previously Presented) The apparatus according to claim 59, wherein the at least
one electronic ticket further includes one or more access limits.

Claim 63: (Previously Presented) The apparatus according to claim 62, wherein the one or
more access limits includes time of day.

Claim 64: (Previously Presented) The apparatus according to claim 62, wherein the one or
more access limits includes authorization to generate further electronic tickets.

Claim 65: (Previously Presented) The apparatus according to claim 59, wherein the at least
one electronic ticket is transmittable to one or more lock devices.

Claim 66: (Previously Presented) The apparatus according to claim 65, wherein said
electronic lock device is a virtual lock device in a form of a software module controlling access
to digital resources.

Claim 67: (Previously Presented) The apparatus according to claim 66, wherein at least one
electronic ticket grants access to at least part of the digital resources.

Claim 68: (Previously Presented) The apparatus according to claim 59, wherein at least one of the apparatus and the electronic key device includes a display for indicating the number of available electronic tickets.

Claim 69: (Previously Presented) The apparatus according to claim 59, wherein the at least one electronic ticket includes an expiration date.

Claim 70: (Previously Presented) The apparatus according to claim 59, wherein the at least one electronic ticket includes a time of day restriction.

Claim 71: (Previously Presented) The apparatus according to claim 70, wherein said additional information contains user-related information.

Claim 72: (Previously Presented) The apparatus according to claim 59, wherein the electronic key device stores additional information unrelated to the private key.

Claim 73: (Previously Presented) The apparatus according to claim 72, wherein said additional information comprises a Social Security number.

Claim 74: (Previously Presented) The apparatus according to claim 59, wherein at least one of the apparatus and the electronic key device includes a personal identification number.

Claim 75: (Previously Presented) The apparatus according to claim 59, wherein at least one of the apparatus, the electronic key device and said electronic lock device includes authentication information in the form of coded information known to a user.

Claim 76: (Previously Presented) The apparatus according to claim 59, wherein at least one of the apparatus, the electronic key device and said electronic lock device includes authentication information in the form of a physical feature of a user.

Claim 77: (Previously Presented) The apparatus according to claim 59, wherein said electronic lock device stores a list of invalid key devices, and denies authorization to any one of the key devices in the list of invalid key devices.

Claim 78: (Previously Presented) The apparatus according to claim 59, wherein said electronic lock device stores a use counter for n-use electronic tickets.

Claim 79: (Previously Presented) The apparatus according to claim 59, wherein said electronic lock device includes an identification number where the identification number is hierarchical in relation to one or more other lock device identification numbers.

Claim 80: (Currently Amended) An apparatus comprising:

a processor configured to:

receive, from a first electronic key device, a ticket comprising a public key of the first electronic key device and a link key configured to authenticate an identity of the apparatus, wherein the link key of the electronic ticket is generated using a one-way hash of a link key of the first electronic key device and a lock identifier of the apparatus, wherein the ticket is generated by a second key device authorized to unlock the apparatus and wherein the ticket is electronically secured by a private key of the second electronic key device,

issue a code to the first electronic key device,

receive an encrypted code corresponding to the issued code encrypted using a private key of the first electronic key device,

determine a decrypted code by decrypting the encrypted code using the public key of the first electronic key device, ~~and~~

determine whether the decrypted code matches the issued code, and

in response to determining that the decrypted code matches the issued code,
unlock the apparatus.

Claim 81: (Previously Presented) The apparatus according to claim 80, wherein the apparatus is a virtual lock device for controlling access to digital resources.

Claim 82: (Previously Presented) The apparatus according to claim 80, wherein at least one of the first and second electronic key devices is not user-interactive.

Claim 83: (Previously Presented) The apparatus according to claim 80, further comprising the second electronic key device, the second electronic key device including a control device configured to load the private key into the second electronic key device remotely and electronically.

Claim 84: (Previously Presented) The apparatus according to claim 83, wherein the control device further loads data into at least one other key device.

Claim 85: (Previously Presented) The apparatus according to claim 83, wherein confirmation data is input into the control device which forwards confirmation to the second electronic key device.

Claims 86-91: (Cancelled).

Claim 92: (Previously Presented) A method comprising:

generating a ticket on a first key device, wherein the first key device is authorized to unlock an electronic lock device, and wherein the ticket includes a public key of a second key device and a link key configured to authenticate an identity of the electronic lock device, wherein the link key of the electronic ticket is generated using a one-way hash of a link key of the first key device and a lock identifier of the electronic lock device;

electronically securing the ticket with a private key of the first key device; and

transmitting the ticket addressed to the second key device, wherein the public key of the second key device is configured to decrypt a code issued by the electronic device and encrypted by the second key device.

Claims 93-94. (Cancelled).

Claim 95: (Previously Presented) The method of claim 92, wherein the first key device is a mobile device.

Claim 96: (Previously Presented) The method of claim 92, wherein the ticket includes one or more use limits.

Claim 97: (Previously Presented) The method of claim 96, wherein the one or more use limits includes a time of day restriction.

Claim 98: (Previously Presented) The method of claim 96, wherein the one or more use limits includes an indication as to whether tickets may be generated by the second key device.

Claim 99: (Previously Presented) A method comprising:

receiving, at a first key device, a ticket from a second key device, wherein the second key device is authorized to unlock an electronic lock device, and wherein the ticket comprises a public key corresponding to the first key device and a link key configured to authenticate an identity of the electronic lock device, wherein the link key of the electronic ticket is generated using a one-way hash of a link key of the second key device and a lock identifier of the electronic lock device and wherein the ticket is secured by a private key of the second key device,

transmitting the ticket addressed to the electronic lock device,

receiving a code issued by the electronic lock device,

encrypting the code using a private key of the first key device, and

transmitting the encrypted code addressed to the electronic lock device.

Claim 100: (Previously Presented) The method of claim 99, wherein the ticket includes one or more use limits.

Claim 101: (Previously Presented) The method of claim 100, wherein the one or more use limits includes a time of day restriction.

Claim 102: (Cancelled).

Claim 103: (Currently Amended) A method comprising:

receiving, from a first electronic key device, a ticket comprising a public key of the first electronic key device and a link key configured to authenticate an identity of an electronic lock device, wherein the link key of the ticket is generated using a one-way hash of a link key of a second electronic key device and a lock identifier of the electronic lock device, wherein the ticket is generated by the second key device authorized to unlock the electronic lock device and wherein the ticket is electronically secured by a private key of the second electronic key device,

issuing a code to the first electronic key device,

receiving an encrypted code corresponding to the code encrypted using a private key of the first electronic key device,

determining a decrypted code by decrypting the encrypted code using the public key of the first electronic key device, ~~and~~

determining whether the decrypted code matches the issued code, and

..... in response to determining that the decrypted code matches the issued code, unlocking the electronic lock device.

Claim 104: (Currently Amended) The method of claim 103, ~~further comprising~~ wherein unlocking the electronic lock device includes unlocking a physical lock device in response to determining that the decrypted code matches the issued code.

Claim 105: (Previously Presented) The method of claim 103, wherein the issued code comprises a number.

Claim 106: (Cancelled).

Claim 107: (Cancelled).

Claim 108: (Currently Amended) One or more computer readable media storing computer readable instructions that, when executed, cause a processor to perform a method comprising:

receiving, from a first electronic key device, a ticket comprising a public key of the first electronic key device and a link key configured to authenticate an identity of an electronic lock device, wherein the link key of the ticket is generated using a one-way hash of a link key of a second electronic key device and a lock identifier of the electronic lock device, wherein the ticket is generated by the second key device authorized to unlock the electronic lock device and wherein the ticket is electronically secured by a private key of the second electronic key device, issuing a code to the first electronic key device,

receiving an encrypted code corresponding to the code encrypted using a private key of the first electronic key device,

determining a decrypted code by decrypting the encrypted code using the public key of the first electronic key device, ~~and~~

determining whether the decrypted code matches the issued code, and

in response to determining that the decrypted code matches the issued code, unlocking the electronic lock device.

Claim 109: (Currently Amended) The one or more computer readable media of claim 108,

~~further comprising instructions for~~ wherein unlocking the electronic lock device includes

unlocking a physical lock device in response to determining that the decrypted code matches the issued code.

Claim 110: (Previously Presented) The one or more computer readable media of claim 108, wherein the issued code comprises a number.

Claim 111: (Previously Presented) One or more computer readable media storing computer readable instructions that, when executed, cause a processor to perform a method comprising:

receiving, at a first key device, a ticket from a second key device, wherein the second key device is authorized to unlock an electronic lock device, and wherein the ticket comprises a

public key corresponding to the first key device and a link key configured to authenticate an identity of the electronic lock device, wherein the link key of the electronic ticket is generated using a one-way hash of a link key of the second key device and a lock identifier of the electronic lock device and wherein the ticket is secured by a private key of the second key device,

transmitting the ticket addressed to the electronic lock device,
receiving a code issued by the electronic lock device,
encrypting the code using a private key of the first key device, and
transmitting the encrypted code addressed to the electronic lock device.

Claim 112: (Previously Presented) The one or more computer readable media of claim 111, wherein the ticket includes one or more use limits.

Claim 113: (Previously Presented) The one or more computer readable media of claim 112, wherein the one or more use limits includes a time of day restriction.

Claim 114: (Previously Presented) One or more computer readable media storing computer readable instructions that, when executed, cause a processor to perform a method comprising:

generating a ticket on a first key device, wherein the first key device is authorized to unlock an electronic lock device, and wherein the ticket includes a public key of a second key device and a link key configured to authenticate an identity of the electronic lock device, wherein the link key of the electronic ticket is generated using a one-way hash of a link key of the first key device and a lock identifier of the electronic lock device;

electronically securing the ticket with a private key of the first key device; and

transmitting the ticket addressed to the second key device, wherein the public key of the second key device is configured to decrypt a code issued by the electronic device and encrypted by the second key device.

Claim 115: (Previously Presented) The one or more computer readable media of claim 114, wherein the first key device is a mobile device.

Claim 116: (Previously Presented) The one or more computer readable media of claim 114, wherein the ticket includes one or more use limits.